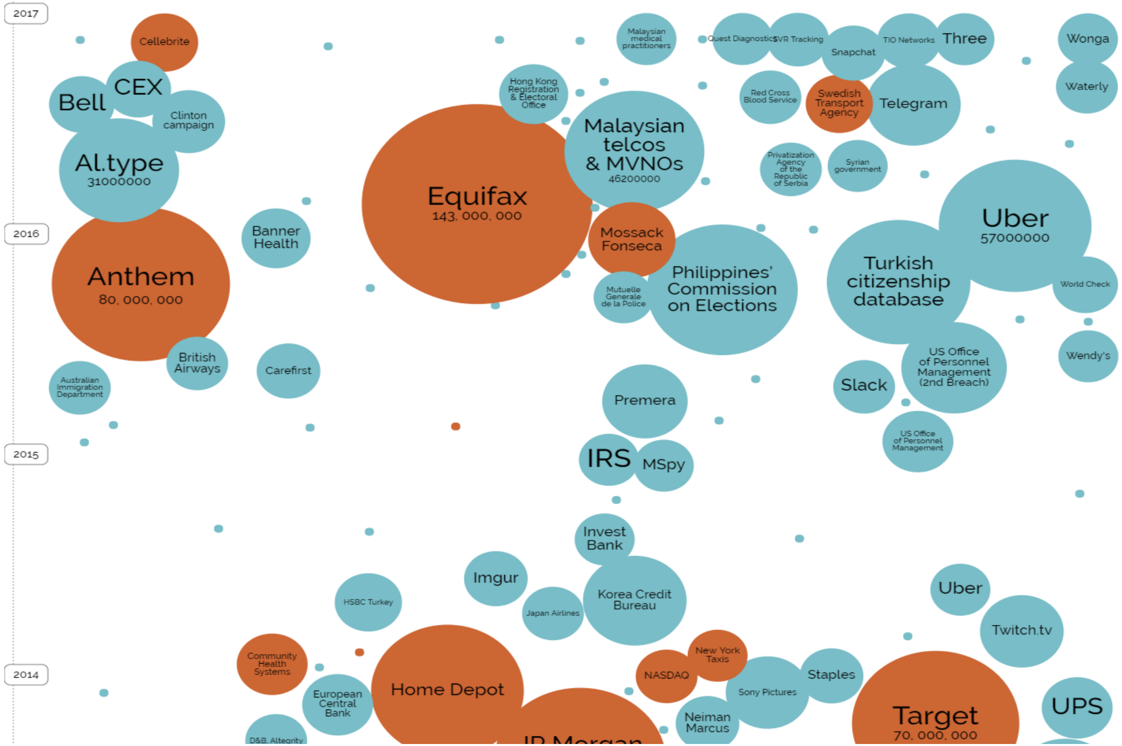
Office of the Secretary of
Public Safety & Homeland Security

Virginia Public Safety Cyber Program

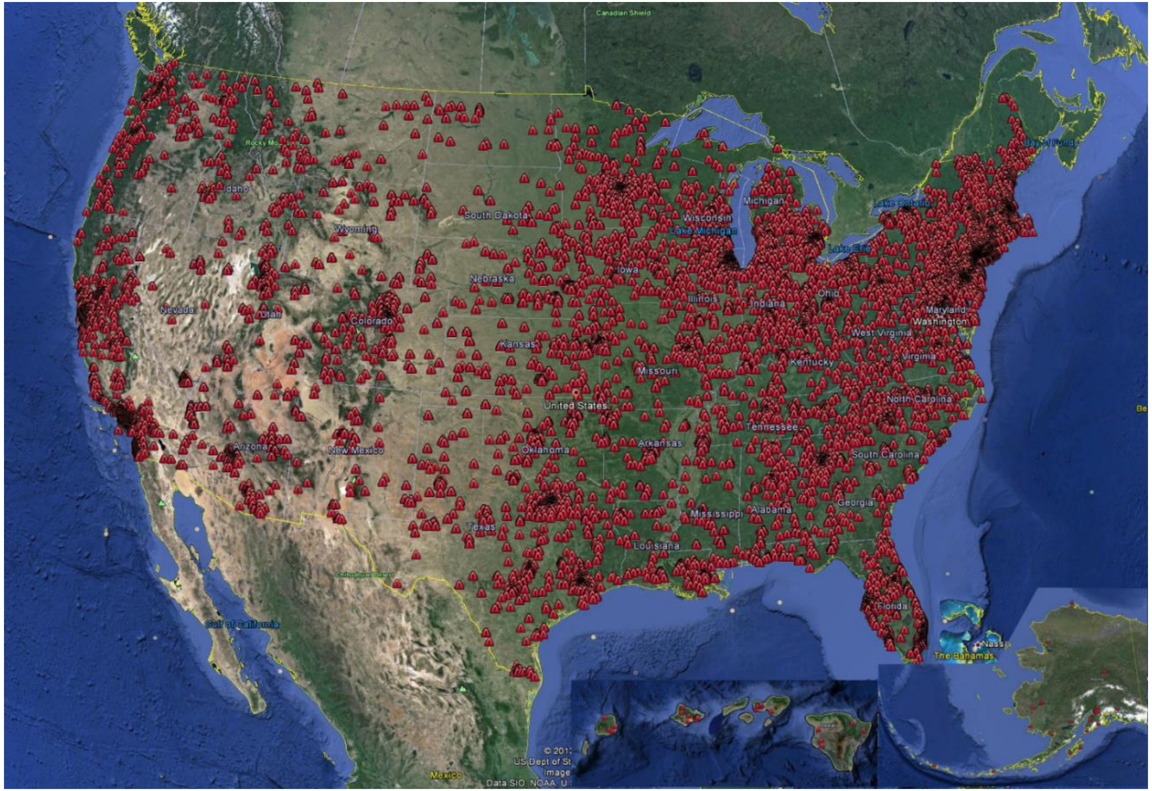
Isaac Janak
Homeland Security and Resilience Staff
Office of the Secretary of Public Safety
& Homeland Security

Office of the Secretary of Public Safety & Homeland Security



Office of the Secretary of Public Safety & Homeland Security

Office of the Secretary of Public Safety & Homeland Security



Threat Actors

لا إله إلا الله
الله
رسول
محمد

Notable Incidents

- October 2016 – Mirai Botnet takes down Dyn DNS
- November 2016 – Russian threat actors target U.S. election systems
- April 2017 – NSA exploits and tools leaked by Shadow Brokers
- May 2017 – WannaCry worldwide ransomware attack
- June 2017 – NotPetya ransomware costs Maersk $300 million in revenue
- December 2017 – TRITON malware shuts down safety control system at critical infrastructure site
- January 2018 – SamSam Ransomware targets Indiana hospital
- March 2018 – Russia identified in targeting of energy and other critical infrastructure sectors
- March 2018 – Ransomware attack shuts down significant portions of Atlanta government
- March 2018 – Ransomware takes down Baltimore 911 dispatching system

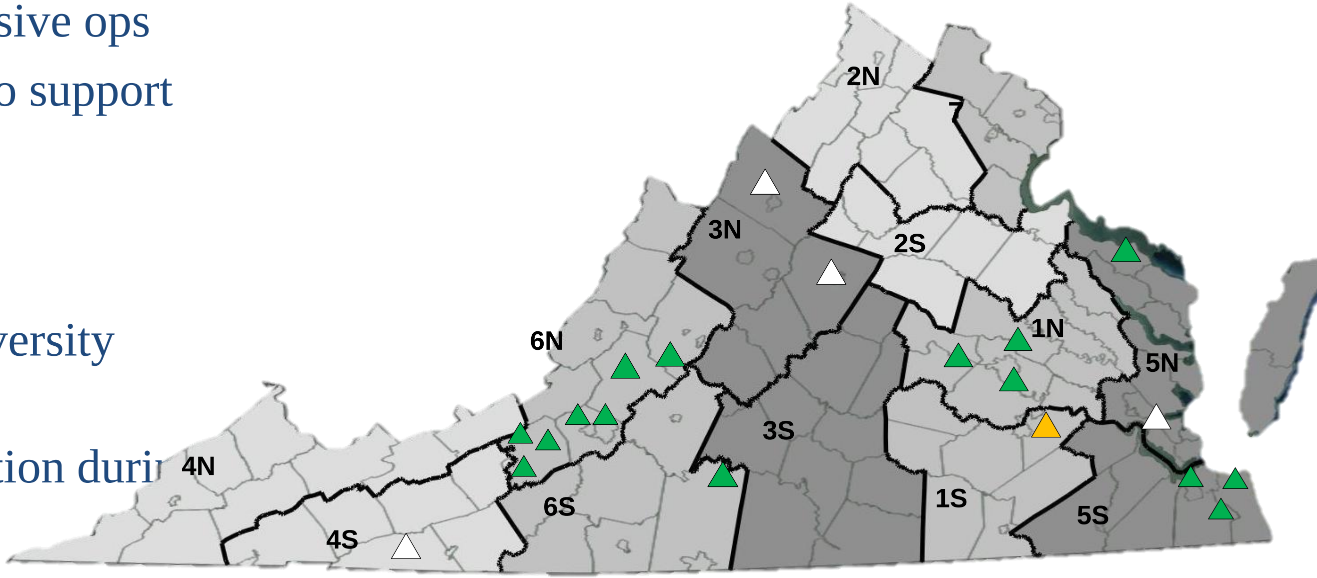
Virginia Public Safety Cyber Initiatives

Virginia Fusion Center – Cyber Intel Unit

- Cyber capability established in 2017
- Composition:
  - 4 analysts
  - 1 special agent
- Purpose – Preparedness & Response:
  - Develop partnerships with public and private sectors to address complex cyber issues
  - Provide intelligence analysis and analytic products
  - Coordinate resources in response to cyber incidents
  - Provide operational support where appropriate to assist with cyber criminal investigations
- Contact: vfc@vsp.virginia.gov

Virginia National Guard

- Home to Nation’s 1st Cyber Brigade capable of assisting the Commonwealth in defensive ops
- Conducted 14 missions to support local and state networks
  - 2 scheduled for 2018
  - 5 in queue for 2019
- Working to develop University partnerships
- Serve as force augmentation duri cyber emergencies



Virginia CERT

- Initially recommended by the Virginia Cyber Security Commission
- Concept: Form a voluntary group of cyber professionals to support preparedness and response activities targeted at local, state, and critical infrastructure organizations
- Public-Private Partnership
- Incentivize with training & skills development opportunities
- Engage Universities to regionalize concept and encourage student/faculty involvement

Local C-SPOC Initiative

- Establishing cyber single point of contact within each locality
  - Developing letter to localities to appoint C-SPOC
- Benefits:
  - Enhanced coordination
    - Law Enforcement & Emergency Management
    - State and federal agencies
  - Access to state and federal resources
  - Cyber incident response coordination
  - Awareness of grant funding opportunities

Critical Infrastructure Cyber Security

Cyber Project Concepts

- Local National Guard Cyber Assessments
  - Competitive applications for local grant share
  - Local or regional project submissions
  - 5 localities have requested assessments for state FY19
  - Project cost estimated $10,000
  - Low sustainment cost
- Exercises – local or regional level
- Cyber Incident Response Plan development
- User awareness and technical training

Cyber Project Guidance

1. Proposals will be reviewed by CSPM in conjunction with Peer Review
2. Projects for equipment/software must include detailed sustainment strategy
3. Proposals should discuss how the project will improve the organization’s security posture and/or lower the risk of incident.
4. It is encouraged that emergency management, law enforcement, and IT staff coordinate on proposal development.
5. Equipment must be categorized by the FEMA Authorized Equipment List

Questions?

Isaac Janak
isaac.janak@governor.virginia.gov